PATENT ABSTRACTS OF JAPAN

(11)Publication number : **2002-335246**

(43)Date of publication of application : **22.11.2002**

(51)Int.Cl. **H04L 12/26**
G06F 13/00
H04L 12/22

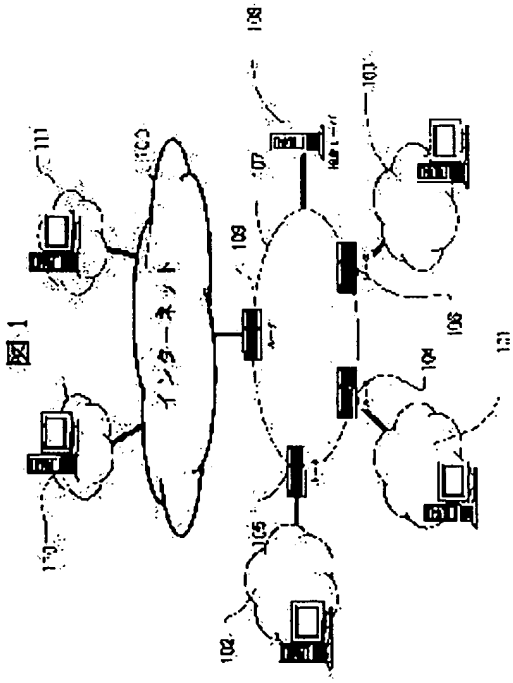
(21)Application number : **2001-139475**

(22)Date of filing : **10.05.2001**

(71)Applicant : **NIPPON TELEGR & TELEPH CORP <NTT>**

(72)Inventor : **ERIC CHEN**
FUJI HITOSHI

(54) METHOD AND DEVICE FOR EXAMINING NETWORK BASE INVASION, PROGRAM FOR NETWORK BASE INVASION EXAMINATION AND RECORDING MEDIUM THEREFOR



(57)Abstract:

PROBLEM TO BE SOLVED: To block an attack from the Internet without introducing network equipment related to security such as a firewall or an IDS(intrusion detection system) and without forcing a burden on a user for acquiring knowledge for operating the introduced network equipment.

SOLUTION: This network base invasion examining method has an examination object data distinguishing step for distinguishing the data of an examination object on the basis of the designation by a user on a network manager side, an attach data investigating step for investigating whether data designated as an examination object are data to be attacked or not and a step for selecting only data which are not to be attacked and data which are not designated as an examination object, from the investigated result and providing such data from the network manager to the user.

CLAIMS

[Claim(s)]

[Claim 1]A network base invasion inspection method comprising:

A subject-of-examination data distinction step which distinguishes data to be examined based on a user's specification by the network operator side.

An attack data survey step which investigates whether data specified as a subject of examination is data which attacks.

A select data offer step which chooses only data which does not deliver an attack, and data which was not specified as a subject of examination from an investigated result and with which a network operator provides a user.

[Claim 2]In order to transmit data which a user specified as a subject of examination to an inspection system in the network base invasion inspection method according to claim 1, A network base invasion inspection method having a routing step which specifies the point which transmits a subject of examination and data to be examined as a router which constitutes a network which a network operator is managing.

[Claim 3]A network base invasion inspection method having an attack inspection central control step which manages intensively an inspection of an attack on two or more users who have connected with a network which a network operator is managing in the network base invasion inspection method according to claim 1.

[Claim 4]Network base invasion test equipment comprising:

A subject-of-examination data distinction means to distinguish data to be examined based on a user's specification by the network operator side.

An attack data survey means to investigate whether data specified as a subject of examination is data which attacks.

A select data providing means which chooses only data which does not deliver an attack, and data which was not specified as a subject of examination from an investigated result and with which a network operator provides a user.

[Claim 5]In order to transmit data which a user specified as a subject of examination to an inspection system in the network base invasion test equipment according to claim 4, Network base invasion test

which a network operator is managing in the network base invasion test equipment according to claim 4.

[Claim 7]It is a program for operating a computer as a system which executes by proxy network base invasion inspection management which is service to a user from a network operator, A subject-of-examination data distinction part which distinguishes data to be examined based on a user's specification, An attack data survey part which investigates whether data specified as a subject of examination is data which attacks, A program operating a computer as a select data providing part which chooses only data which does not deliver an attack, and data which was not specified as a subject of examination from an investigated result, and with which a network operator provides a user.

[Claim 8]It is a program for operating a computer as a system which executes by proxy network base invasion inspection management (processing) which is service to a user from a network operator, A subject-of-examination data distinction part which distinguishes data to be examined based on a user's specification, An attack data survey part which investigates whether data specified as a subject of examination is data which attacks, A select data providing part which chooses only data which does not deliver an attack, and data which was not specified as a subject of examination from an investigated result and with which a network operator provides a user, In order that a user may transmit data specified as a subject of examination to an inspection system, A program, wherein a network operator operates a computer as a router which constitutes a network currently managed as routing parts which specify the point which transmits a subject of examination and data to be examined.

[Claim 9]It is a program for operating a computer as a system which executes by proxy network base invasion inspection management (processing) which is service to a user from a network operator, A subject-of-examination data distinction part which distinguishes data to be examined based on a user's specification, The attack Research and Planning Department which investigates whether data specified as a subject of examination is data which attacks, A select data providing part which chooses only data which does not deliver an attack, and data which was not specified as a subject of examination from an investigated result and with which a network operator provides a user, A program operating a computer as an attack inspection central control department which manages intensively an inspection of attack data to two or more users linked to a network which a network operator is managing (processing).

[Claim 10]A recording medium recording claim 7 thru/or a program indicated in any 1 paragraph in 9.

DETAILED DESCRIPTION

[Detailed Description of the Invention]

[0001]

[Field of the Invention]This invention about the method and device which defend the apparatus connected to the network from the attack from a network, Especially, The network equipment connected to the

[Description of the Prior Art]The attack on the system connected to the Internet is generally classified into a theft, service disturbance, and invasion. The theft of data is performed by being intercepted, while direct access is not carried out to the computer of the owner of data but data goes via the Internet. A service spoiling attack is performed by intercepting the computer which provides service from the user of service. Invasion is performed because an aggressor becomes a computer of an attack target as a regular user and clears up and invades.

[0003]Although the theft of data can prevent the data itself by [advanced] enciphering, it is a firewall and IDS that various methods are examined and the defense method for service disturbance and invasion is most generally used.

[0004]A firewall is a computer system or a router arranged in the middle of connection between the network of a subject of protection, and the Internet, The filtering function has realized control of whether a packet may pass through between the Internet and the networks of a subject of protection / whether there is nothing well. The passage rule of a packet is set as a firewall by items used with transmission destination [of a packet], or transmitting origin or a transmission destination and the group of a transmission source address, and specific application, such as a protocol, a user or an user group, and time.

[0005]IDS is apparatus which can prevent an attack, having a database of the traffic pattern defined for every offensive classification, and analyzing traffic in real time. IDS is introduced into apparatus, such as the phi wall in the node of the Internet, such as a firewall, and the network of a subject of protection, in order to supervise the traffic sent to the network of a subject of protection from the Internet generally. When IDS is detected [the traffic considered to be an attack], while recording the information, An attack is prevented by changing dynamically setting out of packet filtering of the firewall into which IDS is introduced, or the firewall which became independent of IDS set up a priori so that IDS can change setting out.

[0006]

[Problem(s) to be Solved by the Invention]Said firewall and IDS can prevent the attack from the outside delivered from the node to the Internet. As the always-on connecting means of INTANETTOHE, such as ADSL, increases, The personal business company and individual user who are called SOHO (Small Office Home Office), Even if it is a computer which connecting a computer to the Internet everlastingly is increasing and these individuals manage, in that the Internet is always accessed, An attack may be received on a par with the network of the major company protected by a firewall and IDS until now.

[0007]However, the defending means of a firewall or IDS is hard to be introduced into the computer and network which an individual manages for that the introduction cost for purchasing apparatus is high, and the reason advanced knowledge is required for initial setting and employment. Although it was most in the company to station the engineer for employment of a firewall or IDS, it was actually difficult to perform the same measure in an individual user.

[0008]The purpose of this invention introduces the network equipment in connection with security, such as a firewall and IDS. It is in providing the art which can defend the attack from the Internet, without forcing the

[Means for Solving the Problem]It will be as follows if an outline of a typical thing is briefly explained among inventions indicated in this application.

[0011]A subject-of-examination data distinction step from which the 1st invention distinguishes data to be examined based on a user's specification by the network operator side, An attack data survey step which investigates whether data specified as a subject of examination is data which attacks, It is a network base invasion inspection method which has a select data offer step which chooses only data which does not deliver an attack, and data which was not specified as a subject of examination from an investigated result, and with which a network operator provides a user.

[0012]In order that the 2nd invention may transmit data which a user specified as a subject of examination to an inspection system in a network base invasion inspection method of the 1st invention, It has a routing step which specifies the point which transmits a subject of examination and data to be examined as a router which constitutes a network which a network operator is managing.

[0013]The 3rd invention has an attack inspection central control step which manages intensively an inspection of an attack on two or more users linked to a network which a network operator is managing in a network base invasion inspection method of the 1st invention.

[0014]A subject-of-examination data distinction means by which the 4th invention distinguishes data to be examined based on a user's specification by the network operator side, Data specified as a subject of examination possesses a select data providing means which chooses only an attack data survey means to investigate whether it is data which attacks, and data which does not deliver an attack from an investigated result and data which was not specified as a subject of examination and with which a network operator provides a user.

[0015]In order that the 5th invention may transmit data which a user specified as a subject of examination to an inspection system in network base invasion test equipment of the 4th invention, It is network base invasion test equipment possessing a routing step which specifies the point which transmits a subject of examination and data to be examined as a router which constitutes a network which a network operator is managing.

[0016]The 6th invention possesses an attack inspection central control means which processes intensively an inspection of an attack on two or more users linked to a network which a network operator is managing in network base invasion test equipment of the 4th invention.

[0017]The 7th invention is a program for operating a computer as a system which executes by proxy network base invasion inspection management which is service to a user from a network operator, A subject-of-examination data distinction part which distinguishes data to be examined based on a user's specification, An attack data survey part which investigates whether data specified as a subject of examination is data which attacks, It is a program as which a computer is operated as a data selection providing part to which a network operator provides a user only with data which does not deliver an attack from an investigated result, and data which was not specified as a subject of examination

specified as a subject of examination is data which attacks, A data selection providing part which chooses only data which does not deliver an attack, and data which was not specified as a subject of examination from an investigated result and with which a network operator provides a user, In order that a user may transmit data specified as a subject of examination to an inspection system, it is a program to which a network operator operates a computer as a router which constitutes a network currently managed as routing parts which specify the point which transmits a subject of examination and data to be examined.

[0019]The 9th invention is a program for operating a computer as a system which executes by proxy network base invasion inspection management (processing) which is service to a user from a network operator, A subject-of-examination data distinction part which distinguishes data to be examined based on a user's specification, The attack Research and Planning Department which investigates whether data specified as a subject of examination is data which attacks, A select data providing part which chooses only data which does not deliver an attack, and data which was not specified as a subject of examination from an investigated result and with which a network operator provides a user, It is a program as which a computer is operated as an attack inspection central control department which manages intensively an inspection of attack data to two or more users linked to a network which a network operator is managing (processing).

[0020]The 10th invention is the recording medium which recorded any one program among said 7th [the] thru/or the 9th invention.

[0021]That is, in this invention, it is a premise that network equipment in connection with security, such as a firewall and IDS, is installed in an Internet Service Provider's (ISP) network instead of a user's network. In other words, it is wide opened from a user purchasing and maintaining network equipment in connection with security by this for ISP implementing a measure in connection with security instead of a user.

[0022]ISP manages a means to protect a network of a user who has connected, intensively. That is, a user linked to ISP specifies routing information reflecting conditions to be examined registered a priori as a router (edge router) which has connected a network of ISP, and the other network.

[0023]It is transmitting data sent from the transmitting origin which, as for this routing information, a user specified as a subject of examination to an inspection system, and transmitting to a user data sent from the transmitting origin which a user does not specify as a subject of examination, Invasion can be inspected about a subject of examination which a user wishes. For this reason, routing of all the edge routers which constitute a network of ISP is managed intensively, An attack from other users linked to ISP to a network of a user linked to ISP can also cancel ISP, before an attack from external networks, such as the Internet, also reaches a user's network.

[0024]By distinguishing a network which a user trusts from the other network as a way a user specifies an offensive subject of examination, Data sent from the other network inspects, and after safety is confirmed, a user enables it for a direct user to enable it to receive data transmitted from a reliable network, and to receive it. Time which processing which will be performed by the time a user receives without checking data sent by this from a network to trust for invasion detection decreases, and is required is shortened

[0027]

[Invention embodiment] Drawing 1 is a mimetic diagram showing a topology of a network concerning this invention. As shown in drawing 1, it is connected to the network 107 of ISP via the routers 104, 105, and 106, respectively, and a user's networks 101, 102, and 103 are connected also with the inspection server 108 which applied a network base invasion inspection method and a device of this invention. The network 107 of ISP is connected with the Internet 100 via the router 109. Furthermore, the terminal 110 and the terminal 111 are terminals located in somewhere on the Internet 100.

[0028]In a network like drawing 1, drawing 2 shows an outline of a flow of traffic realized by this invention. As for the terminal 201 which receives data from the Internet 100, the terminal 202 transmits data from the reliable network 212, and the terminal 203 will identify it, if data is transmitted from the network 213 which is not reliable.

[0029]The router 204 will be transmitted to the receiving terminal 201 of data as it is, if data from the reliable terminal 202 which belongs to the reliable network 212 is received. on the other hand -- the router 204 -- true character -- when data from the unknown network 213, i.e., a network which is not reliable, is received, the data is transmitted to the inspection server 205. Data transmitted to the inspection server 205 is inspected, when it is considered as a result of an inspection that it is safe data, the data is transmitted to the terminal 201, and as a result of an inspection, when it is considered that it is not safe data, it is canceled.

[0030]Drawing 3 shows other data flow in a network of drawing 1. A case where data is received from a terminal connected to ISP networks 107 where the receiving terminal 301 of data is the same shows by this drawing 3, The terminal 302 transmits data from the reliable network 312, and the terminal 303 will identify it, if data is transmitted from the network 313 which is not reliable. If the router 304 receives data from the terminal 302, received data will be transmitted to the terminal 301.

[0031]On the other hand, the router 305 will transmit received data to the inspection server 306, if data from the terminal 303 is received. Data transmitted to the inspection server 306 is inspected, when it is considered as a result of an inspection that it is safe data, the data is transmitted to the terminal 301, and as a result of an inspection, when it is considered that it is not safe data, it is canceled.

[0032]Drawing 4 is a figure showing functional constitution of an inspection server which mounted this invention. The communications channel 401 expresses LAN (Local Area Network) and other transit networks. Data divided into a packet or data which is not divided is received by the network driver 402 via the communications channel 401.

[0033]The network driver 402 comprises hardware or software, hardware, and software, receives data from the communications channel 401, and changes it into a gestalt which can decode a computer. The network driver 402 is delivered to the data analysis part 403 which analyzes data to receive data in real time.

[0034]The data analysis part 403 comprises the user policy execution part 404 and the invasion defense part 405. The user policy execution part 404 determines whether cancel data which received from a network

level here. Data which was not canceled by the user policy execution part 404 wins popularity to the invasion defense part 405, and is passed to it. The invasion defense part 405 judges whether data is safe with reference to the invasion pattern database 407 with which offensive data is defined. The subscriber management department 408 has managed the user databases 406. When a user's data registered into the user databases 406 is changed, the routing Management Department 409 notifies change of routing information to an edge router (equivalent to the routers 104, 105, 106, and 109 in the case of the network 107 of ISP of drawing 1).

[0036]Drawing 5 is a figure for explaining how to determine the point which transmits data which an edge router received. There is the access table 502 in each edge router, two kinds of information are indicated in this table, and an address which shows a network trusted for every service subscriber of the network 107 of ISP is written. The "member" column expresses a member who wishes to inspect, and an addresser who receives data is expressed, without inspecting in the "trusting agency" column.

[0037]Drawing 6 is a flow chart for explaining an example of processing of a router (edge router) currently installed in a boundary of a network of ISP and other networks which are managed by inspection server which applied this invention.

[0038]Below, data sent to a network of ISP is called inflow data to ISP from a network of a user using the Internet or ISP.

[0039]An edge router will judge whether it is data transmitted to a subscriber to inspection service with reference to an access table, if inflow data to ISP is received (s101) (s102). When data is not data transmitted to a subscriber to inspection service, it transmits toward an addressee (s104). On the contrary, in the case of data in which data is transmitted to a subscriber to inspection service, it is investigated whether an edge router is a sending person who belongs to a network which a sending person of data can trust and who can trust it (s103).

[0040]In being a sending person whom a sending person of data can trust, it transmits data to an addressee, and when it is a sending person whom a sending person of data cannot trust, cis- TEMUHE data which inspects data is transmitted (s105).

[0041]Drawing 7 is a flow chart for explaining an example of processing of a system which inspects data with the application of this invention. If data is received from an edge router (s201), an inspection system of data, A security level which a user registered into beforehand from user databases is searched (s202), and received data confirms whether to have agreed in a security level searched from user databases (s203). Data is canceled when not having agreed in a security level which a user registered a priori as a result of a check (s204), When having agreed in a security level which a user registered a priori, an inspection system searches a pattern of invasion which IDS holds (s205), and analyzes the danger of received data. When an analysis result of data is judged to be data for invading, (s206) and data of those are canceled (s204), and when that is not right, it is transmitted to an addressee (s207).

[0042]Drawing 8 is the data which recorded operation of an inspection system which applied this invention

since it turns out that ISP is attacking an inspection service subscriber in order, it becomes possible to give a user linked to ISP which has not received an attack an alarm, or to give him more effective management.

[0043]As mentioned above, as for this invention, although an invention made by this invention person was concretely explained based on said embodiment, it is needless to say for it to be able to change variously in a range which is not limited to said embodiment and does not deviate from the gist.

[0044]

[Effect of the Invention]It will be as follows if the effect acquired by the typical thing among the inventions indicated in this application is explained briefly. According to this invention, the user using a network becomes available about the security solution provided by ISP used when accessing the Internet, without installing the network equipment in connection with security oneself.

[0045]That is, the attack via a network can be prevented, without [without it purchases hardware and software for defense of a user's attack, and] mastering the knowledge which employs those hardwares and software.

[0046]In the position of ISP, this invention can be provided as added value of service of ISP.

[0047]In defending an attack like DDoS (Distributed Denial of Service) which consumes a network zone, According to this invention, it can make it possible for ISP not to pass the traffic which is sent from the upstream of a network topology and which is not preferred, and a zone for a user to connect with external networks, such as the Internet, by this can be secured now.

[0048]Since network operators, such as ISP, provide offensive inspection service by the system managed intensively at one place, compared with the user conducting the individual and same attack inspection, the range which can collect the records on which an attack was delivered spreads in whole ISP. For this reason, the new information which was not found only by individual record may be acquired.

[Translation done.]

(19)日本国特許庁（ＪＰ）　(12)**公開特許公報**（Ａ）　(11)特許出願公開番号
特開2002－335246
（P2002－335246A）
(43)公開日　平成14年11月22日(2002.11.22)

(51)Int.Cl.[7]	識別記号	Ｆ Ｉ		テーマコード（参考）
Ｈ０４Ｌ　12/26		Ｈ０４Ｌ　12/26		５Ｂ０８９
Ｇ０６Ｆ　13/00	３５１	Ｃ０６Ｆ　13/00	３５１Ｚ	５Ｋ０３０
Ｈ０４Ｌ　12/22		Ｈ０４Ｌ　12/22		

審査請求　未請求　請求項の数10　ＯＬ　（全 12 頁）

(21)出願番号　特願2001－139475(P2001－139475)
(22)出願日　平成13年５月10日(2001.5.10)

(71)出願人　000004226
日本電信電話株式会社
東京都千代田区大手町二丁目３番１号
(72)発明者　エリック　チェン
東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内
(72)発明者　冨士　仁
東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内
(74)代理人　100083552
弁理士　秋田　収喜　（外１名）

最終頁に続く

(54)【発明の名称】　ネットワークベース侵入検査方法及び装置並びにネットワークベース侵入検査用プログラム及びその記録媒体

(57)【要約】
【課題】　ファイアウォールやＩＤＳといったセキュリティに係るネットワーク機器を導入することや、導入したネットワーク機器を運用するための知識を獲得するという負担をユーザに強いることなく、インターネットからの攻撃を防御する。
【解決手段】　ネットワーク運営者側でユーザの指定に基づいて検査対象のデータを区別する検査対象データ区別ステップと、検査対象と指定されたデータは攻撃を行うデータか否かを調査する攻撃データ調査ステップと、調査した結果から攻撃を行わないデータと検査対象と指定されなかったデータだけを選択してネットワーク運営者がユーザに提供するステップとを有するネットワークベース侵入検査方法である。

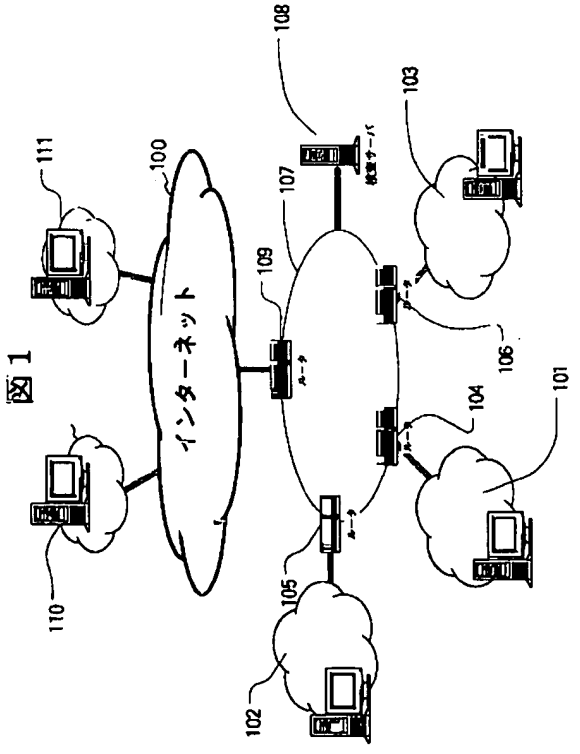


図１

【特許請求の範囲】

【請求項１】　ネットワーク運営者側でユーザの指定に基づいて検査対象のデータを区別する検査対象データ区別ステップと、検査対象と指定されたデータは攻撃を行うデータか否かを調査する攻撃データ調査ステップと、調査した結果から攻撃を行わないデータと検査対象と指定されなかったデータだけを選択してネットワーク運営者がユーザに提供する選択データ提供ステップとを有することを特徴とするネットワークベース侵入検査方法。

【請求項２】　請求項１に記載のネットワークベース侵入検査方法において、ユーザが検査対象と指定したデータを検査システムに転送するために、ネットワーク運営者が運営しているネットワークを構成するルータに検査対象及び検査対象のデータを転送する先を指定しておくルーティングステップを有することを特徴とするネットワークベース侵入検査方法。

【請求項３】　請求項１に記載のネットワークベース侵入検査方法において、ネットワーク運営者が運営しているネットワークに接続している複数のユーザに対する攻撃の検査を集中的に管理する攻撃検査集中管理ステップを有することを特徴とするネットワークベース侵入検査方法。

【請求項４】　ネットワーク運営者側でユーザの指定に基づいて検査対象のデータを区別する検査対象データ区別手段と、検査対象と指定されたデータは攻撃を行うデータか否かを調査する攻撃データ調査手段と、調査した結果から攻撃を行わないデータと検査対象と指定されなかったデータだけを選択してネットワーク運営者がユーザに提供する選択データ提供手段とを具備することを特徴とするネットワークベース侵入検査装置。

【請求項５】　請求項４に記載のネットワークベース侵入検査装置において、ユーザが検査対象と指定したデータを検査システムに転送するために、ネットワーク運営者が運営しているネットワークを構成するルータに検査対象及び検査対象のデータを転送する先を指定しておくルーティングステップを具備することを特徴とするネットワークベース侵入検査装置。

【請求項６】　請求項４に記載のネットワークベース侵入検査装置において、ネットワーク運営者が運営しているネットワークに接続している複数のユーザに対する攻撃データの検査を集中的に管理する集中的検査管理手段を具備することを特徴とするネットワークベース侵入検査装置。

【請求項７】　ネットワーク運営者からユーザへのサービスであるネットワークベース侵入検査管理を代行するシステムとしてコンピュータを機能させるためのプログラムであって、ユーザの指定に基づいて検査対象のデータを区別する検査対象データ区別部と、検査対象と指定されたデータは攻撃を行うデータか否かを調査する攻撃データ調査部と、調べた結果から攻撃を行わないデータと検査対象と指定されなかったデータだけを選択してネットワーク運営者がユーザに提供する選択データ提供部としてコンピュータを機能させることを特徴とするプログラム。

【請求項８】　ネットワーク運営者からユーザへのサービスであるネットワークベース侵入検査管理（処理）を代行するシステムとしてコンピュータを機能させるためのプログラムであって、ユーザの指定に基づいて検査対象のデータを区別する検査対象データ区別部と、検査対象と指定されたデータは攻撃を行うデータか否かを調査する攻撃データ調査部と、調査した結果から攻撃を行わないデータと検査対象と指定されなかったデータだけを選択してネットワーク運営者がユーザに提供する選択データ提供部と、ユーザが検査対象と指定したデータを検査システムに転送するために、ネットワーク運営者が、運営しているネットワークを構成するルータに検査対象及び検査対象のデータを転送する先を指定しておくルーティング部としてコンピュータを機能させることを特徴とするプログラム。

【請求項９】　ネットワーク運営者からユーザへのサービスであるネットワークベース侵入検査管理（処理）を代行するシステムとしてコンピュータを機能させるためのプログラムであって、ユーザの指定に基づいて検査対象のデータを区別する検査対象データ区別部と、検査対象と指定されたデータは攻撃を行うデータか否かを調査する攻撃調査部と、調査した結果から攻撃を行わないデータと検査対象と指定されなかったデータだけを選択してネットワーク運営者がユーザに提供する選択データ提供部と、ネットワーク運営者が運営しているネットワークに接続している複数のユーザに対する攻撃データの検査を集中的に管理（処理）する攻撃検査集中管理部としてコンピュータを機能させることを特徴とするプログラム。

【請求項１０】　請求項７乃至９うちいずれか１項に記載されたプログラムを記録したことを特徴とする記録媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、ネットワークに接続された機器をネットワークからの攻撃から防御する方法及び装置に関し、特に、インターネットに接続されたネットワーク機器をルータ経路制御とＩＤＳ（侵入検知システム：Intrusion Detection System）技術またはファイアウォールによって防御する方法に係る攻撃の防止方法及び装置並びにプログラムを記録した記録媒体に関する。

【０００２】

【従来の技術】インターネットに接続されているシステムに対する攻撃は、一般的に盗難、サービス妨害、侵入に分類される。データの盗難は、データの所有者のコン

ピュータに直接アクセスするのではなく、データがインターネットを経由している間に盗聴されることで行われる。サービス妨害攻撃は、サービスの利用者からサービスを提供するコンピュータを遮断してしまうことによって行われる。侵入は、攻撃者が攻撃目標のコンピュータに正規のユーザとしてなりすまして侵入することで行われる。

【０００３】データの盗難はデータ自体を高度の暗号化することによって防ぐことができるが、サービス妨害及び侵入に対する防御方法は様々な方法が検討されており、最も一般的に利用されているのはファイアウォールとＩＤＳである。

【０００４】ファイアウォールは、保護対象のネットワークとインターネットとの接続の中間に配置されるコンピュータシステムまたはルータ等であり、パケットがインターネットと保護対象のネットワークの間を通過して良いか／良くないかの制御をフィルタリング機能によって実現している。パケットの通過規則は、パケットの送信先または送信元あるいは送信先及び送信元アドレスの組、特定のアプリケーションで使われるプロトコル、ユーザあるいはユーザグループ、時間などの項目によってファイアウォールに設定される。

【０００５】ＩＤＳは、攻撃の種別ごとに定義されたトラフィックパターンのデータベースを持ち、トラフィックをリアルタイムに分析しながら攻撃を防ぐことができる機器である。ＩＤＳは一般的に、インターネットから保護対象のネットワークへ送られてくるトラフィックを監視するために、ファイアウォールなどインターネットと保護対象のネットワークとの接続点にあるファイウォールなどの機器に導入される。ＩＤＳは、攻撃と思われるトラフィックを検出した場合、その情報を記録するとともに、ＩＤＳが導入されているファイアウォール、またはＩＤＳが設定を変更できるように事前に設定されているＩＤＳと独立したファイアウォールのパケットフィルタリングの設定を動的に変更することで攻撃を防ぐ。

【０００６】

【発明が解決しようとする課題】前記ファイアウォールとＩＤＳはインターネットへの接続点から行われる外部からの攻撃を防ぐことができる。ＡＤＳＬ等のインターネットへの常時接続手段が増えてくるにしたがって、ＳＯＨＯ（Ｓmall Office Home Office）と呼ばれる個人事業者や個人ユーザが、コンピュータをインターネットに恒久的に接続しておくことが増えてきており、これら個人が管理するコンピュータであっても、インターネットへ常に接続しているという点で、これまでファイアウォールやＩＤＳによって守られていた大企業のネットワークと同等に攻撃を受ける可能性がある。

【０００７】しかし、ファイアウォールやＩＤＳの防御手段は、機器を購入するための導入コストが高いということと、初期設定及び運用に高度な知識が必要という理由で個人が管理するコンピュータやネットワークには導入されにくい。実際、企業ではファイアウォールやＩＤＳの運用のために技術者を配置していることがほとんどであるが、個人ユーザ等では、同様の対策を行うことは困難であった。

【０００８】本発明の目的は、ファイアウォールやＩＤＳといったセキュリティに関わるネットワーク機器を導入することや、導入したネットワーク機器を運用するための知識を獲得するという負担をユーザに強いることなく、インターネットからの攻撃を防御することができる技術を提供することにある。

【０００９】本発明の前記ならびにその他の目的と新規な特徴は、本明細書の記述及び添付図面によって明らかにする。

【００１０】

【課題を解決するための手段】本願において開示される発明のうち代表的なものの概要を簡単に説明すれば下記のとおりである。

【００１１】第１の発明は、ネットワーク運営者側でユーザの指定に基づいて検査対象のデータを区別する検査対象データ区別ステップと、検査対象と指定されたデータは攻撃を行うデータか否かを調査する攻撃データ調査ステップと、調査した結果から攻撃を行わないデータと検査対象と指定されなかったデータだけを選択してネットワーク運営者がユーザに提供する選択データ提供ステップとを有するネットワークベース侵入検査方法である。

【００１２】第２の発明は、前記第１の発明のネットワークベース侵入検査方法において、ユーザが検査対象と指定したデータを検査システムに転送するために、ネットワーク運営者が運営しているネットワークを構成するルータに検査対象及び検査対象のデータを転送する先を指定しておくルーティングステップを有するものである。

【００１３】第３の発明は、前記第１の発明のネットワークベース侵入検査方法において、ネットワーク運営者が運営しているネットワークに接続している複数のユーザに対する攻撃の検査を集中的に管理する攻撃検査集中管理ステップを有するものである。

【００１４】第４の発明は、ネットワーク運営者側でユーザの指定に基づいて検査対象のデータを区別する検査対象データ区別手段と、検査対象と指定されたデータは攻撃を行うデータか否かを調査する攻撃データ調査手段と、調査した結果から攻撃を行わないデータと検査対象と指定されなかったデータだけを選択してネットワーク運営者がユーザに提供する選択データ提供手段とを具備するものである。

【００１５】第５の発明は、前記第４の発明のネットワークベース侵入検査装置において、ユーザが検査対象と指定したデータを検査システムに転送するために、ネッ

トワーク運営者が運営しているネットワークを構成するルータに検査対象及び検査対象のデータを転送する先を指定しておくルーティングステップを具備するネットワークベース侵入検査装置である。

【００１６】第６の発明は、前記第４の発明のネットワークベース侵入検査装置において、ネットワーク運営者が運営しているネットワークに接続している複数のユーザに対する攻撃の検査を集中的に処理する攻撃検査集中管理手段を具備するものである。

【００１７】第７の発明は、ネットワーク運営者からユーザへのサービスであるネットワークベース侵入検査管理を代行するシステムとしてコンピュータを機能させるためのプログラムであって、ユーザの指定に基づいて検査対象のデータを区別する検査対象データ区別部と、検査対象と指定されたデータは攻撃を行うデータか否かを調査する攻撃データ調査部と、調査した結果から攻撃を行わないデータと検査対象と指定されなかったデータだけをネットワーク運営者がユーザに提供するデータ選択提供部としてコンピュータを機能させるプログラムである。

【００１８】第８の発明は、ネットワーク運営者からユーザへのサービスであるネットワークベース侵入検査管理（処理）を代行するシステムとしてコンピュータを機能させるためのプログラムであって、ユーザの指定に基づいて検査対象のデータを区別する検査対象データ区別部と、検査対象と指定されたデータは攻撃を行うデータか否かを調査する攻撃調査部と、調査した結果から攻撃を行わないデータと検査対象と指定されなかったデータだけを選択してネットワーク運営者がユーザに提供するデータ選択提供部と、ユーザが検査対象と指定したデータを検査システムに転送するために、ネットワーク運営者が、運営しているネットワークを構成するルータに検査対象及び検査対象のデータを転送する先を指定しておくルーティング部としてコンピュータを機能させるプログラムである。

【００１９】第９の発明は、ネットワーク運営者からユーザへのサービスであるネットワークベース侵入検査管理（処理）を代行するシステムとしてコンピュータを機能させるためのプログラムであって、ユーザの指定に基づいて検査対象のデータを区別する検査対象データ区別部と、検査対象と指定されたデータは攻撃を行うデータか否かを調査する攻撃調査部と、調査した結果から攻撃を行わないデータと検査対象と指定されなかったデータだけを選択してネットワーク運営者がユーザに提供する選択データ提供部と、ネットワーク運営者が運営しているネットワークに接続している複数のユーザに対する攻撃データの検査を集中的に管理（処理）する攻撃検査集中管理部としてコンピュータを機能させるプログラムである。

【００２０】第１０の発明は、前記第７乃至第９の発明のうちいずれか１つのプログラムを記録した記録媒体である。

【００２１】すなわち、本発明では、ファイアウォールやＩＤＳといったセキュリティに関わるネットワーク機器は、ユーザのネットワークではなく、インターネットサービスプロバイダ（ＩＳＰ）のネットワークに設置されていることが前提である。言い換えれば、ユーザに代わってＩＳＰがセキュリティに関わる対策を実施することを対象としており、これによって、ユーザはセキュリティに関わるネットワーク機器を購入、維持することから開放される。

【００２２】ＩＳＰは接続しているユーザのネットワークを保護する手段を集中的に管理する。すなわち、ＩＳＰのネットワークとそれ以外のネットワークを接続しているルータ（エッジルータ）には、ＩＳＰに接続しているユーザが事前に登録した検査対象の条件を反映したルーティング情報を指定しておく。

【００２３】このルーティング情報は、ユーザが検査対象に指定した送信元から送られてきたデータは検査システムに転送し、ユーザが検査対象に指定していない送信元から送られてきたデータはユーザに転送することで、ユーザが希望する検査対象について侵入の検査を実施することができる。このために、ＩＳＰのネットワークを構成するすべてのエッジルータのルーティングを集中的に管理し、ＩＳＰに接続しているユーザのネットワークに対するＩＳＰに接続している他のユーザからの攻撃も、インターネット等の外部ネットワークからの攻撃も、ユーザのネットワークに到達する前にＩＳＰが破棄することができる。

【００２４】ユーザが攻撃の検査対象を指定する方法として、ユーザが信頼するネットワークをそれ以外のネットワークと区別することによって、信頼できるネットワークから送信されてきたデータは直接ユーザが受信できるようにし、それ以外のネットワークから送られてきたデータは検査を行い、安全性が確かめられてからユーザが受信できるようにする。これにより、信頼するネットワークから送られてきたデータは、侵入検知のためのチェックを受けずにユーザが受信するまでに行われる処理が減少すると共に要する時間が短縮される。

【００２５】ユーザが受信する意思のあるパケットのポート番号の集合をセキュリティレベルとして指定することによって、指定されていないポート番号へ向けて送信されているパケットを破棄することができる。

【００２６】以下、本発明について、図面を参照して本発明の実施の形態（実施例）とともに詳細に説明する。

【００２７】

【発明実施の形態】図１は、本発明に係るネットワークの接続形態を示す模式図である。図１に示すように、ユーザのネットワーク１０１、１０２、１０３は、それぞれルータ１０４、１０５、１０６を経由してＩＳＰのネ

ットワーク１０７に接続され、本発明のネットワークベース侵入検査方法及び装置を適用した検査サーバ１０８とも接続されている。ＩＳＰのネットワーク１０７は、ルータ１０９を経由してインターネット１００と接続されている。さらに端末１１０及び端末１１１はインターネット１００上のどこかに位置する端末である。

【００２８】図2は、図1のようなネットワークにおいて、本発明によって実現されるトラフィックの流れの概要を示している。インターネット１００からのデータを受信する端末２０１は、端末２０２は信頼できるネットワーク２１２からデータを送信し、端末２０３は信頼できないネットワーク２１３からデータを送信していると識別している。

【００２９】ルータ２０４は信頼できるネットワーク２１２に所属している信頼できる端末２０２からのデータを受け取ると、そのままデータの受信端末２０１へ転送する。一方、ルータ２０４が正体不明のネットワーク、すなわち、信頼できないネットワーク２１３からのデータを受信した場合、そのデータを検査サーバ２０５へ転送する。検査サーバ２０５へ転送されたデータを検査し、検査の結果、安全なデータだとみなされた場合、そのデータは端末２０１へ転送され、検査の結果、安全なデータではないとみなされた場合は破棄される。

【００３０】図3は、図1のネットワークにおける他のデータの流れを示している。この図3で示しているのは、データの受信端末３０１が同じＩＳＰネットワーク１０７に接続されている端末からデータを受信する場合であり、端末３０２は信頼できるネットワーク３１２からデータを送信し、端末３０３は信頼できないネットワーク３１３からデータを送信していると識別している。ルータ３０４が端末３０２からデータを受信すると、受信したデータは端末３０１へ転送される。

【００３１】一方、ルータ３０５は端末３０３からのデータを受信すると、受信したデータを検査サーバ３０６へ転送する。検査サーバ３０６へ転送されたデータを検査し、検査の結果、安全なデータだとみなされた場合、そのデータは端末３０１へ転送され、検査の結果、安全なデータではないとみなされた場合は破棄される。

【００３２】図4は、本発明を実装した検査サーバの機能構成を示す図である。通信チャネル４０１はＬＡＮ（Local Area Network）や他の中継ネットワークを表している。パケットに分割されたデータ、または分割されていないデータは、通信チャネル４０１を経由してネットワークドライバ４０２によって受信される。

【００３３】ネットワークドライバ４０２は、ハードウェアまたはソフトウェア、及びハードウェア及びソフトウェアで構成され、通信チャネル４０１からデータを受信しコンピュータが解読可能な形態に変換する。また、ネットワークドライバ４０２は、データを受信するとリアルタイムにデータを分析するデータ分析部４０３へ受け渡す。

【００３４】データ分析部４０３はユーザポリシ実行部４０４と侵入防御部４０５から構成される。ユーザポリシ実行部４０４は、ユーザが事前に登録してあるセキュリティのレベルを保存してあるユーザデータベース４０６を参照し、ネットワークドライバから受け渡されたデータを破棄するか否かを決定する。

【００３５】ここでのセキュリティレベルとは、「高中低」という３段階程度で表すこともでき、それぞれの程度ごとに受信したデータを破棄するか否かという検査をする項目の数や厳しさが異なる。ユーザポリシ実行部４０４によって破棄されなかったデータは、侵入防御部４０５へ受け渡される。侵入防御部４０５は、攻撃のデータが定義してある侵入パターンデータベース４０７を参照し、データが安全であるか否かを判定する。加入者管理部４０８はユーザデータベース４０６を管理している。ユーザデータベース４０６に登録されているユーザのデータが変更された場合、ルーティング管理部４０９はエッジルータ（図1のＩＳＰのネットワーク１０７の場合には、ルータ１０４、１０５、１０６、１０９に相当）にルーティング情報の変更を通知する。

【００３６】図5は、エッジルータが受信したデータを転送する先を決定する方法を説明するための図である。各エッジルータにはアクセステーブル５０２があり、このテーブルには２種類の情報が記載されており、ＩＳＰのネットワーク１０７のサービス加入者ごとに信頼するネットワークを示すアドレスが書かれている。「加入者」欄は検査を希望する加入者を表し、「信頼元」欄には検査をすることなくデータを受信する発信者を表す。

【００３７】図6は、本発明を適用した検査サーバによって管理されるＩＳＰのネットワークとその他のネットワークとの境界に設置されているルータ（エッジルータ）の処理例を説明するためのフローチャートである。

【００３８】以下では、インターネットまたはＩＳＰを利用しているユーザのネットワークから、ＩＳＰのネットワークへ送られてくるデータをＩＳＰへの流入データという。

【００３９】エッジルータは、ＩＳＰへの流入データを受信すると（ｓ１０１）、アクセステーブルを参照し、検査サービスの加入者へ送信されているデータか否かを判断する（ｓ１０２）。データが検査サービスの加入者へ送信されているデータではない場合は、受信者へ向かって転送する（ｓ１０４）。逆に、データが検査サービスの加入者へ送信されているデータの場合は、エッジルータはデータの送信者が信頼できるネットワークに所属している信頼できる送信者であるか否かを調べる（ｓ１０３）。

【００４０】データの送信者が信頼できる送信者である場合には、受信者へデータを転送し、データの送信者が信頼できない送信者である場合は、データの検査を行う

システムへデータを転送する（ｓ１０５）。

【００４１】図7は、本発明を適用してデータの検査を行うシステムの処理例を説明するためのフローチャートである。データの検査システムは、エッジルータからデータを受信すると（ｓ２０１）、ユーザデータベースから事前にユーザが登録したセキュリティレベルを検索し（ｓ２０２）、受信したデータがユーザデータベースから検索されたセキュリティレベルに合致しているかをチェックする（ｓ２０３）。チェックの結果、ユーザが事前に登録したセキュリティレベルに合致していない場合にはデータを破棄し（ｓ２０４）、ユーザが事前に登録したセキュリティレベルに合致している場合には、検査システムはＩＤＳが保持している侵入のパターンを検索し（ｓ２０５）、受信したデータの危険性を分析する。データの分析結果が、侵入を行うためのデータであると判断された場合には（ｓ２０６）、そのデータは破棄され（ｓ２０４）、そうでない場合には受信者へ転送される（ｓ２０７）。

【００４２】図8は、本発明を適用した検査システムの動作を記録したデータであり、８０１、８０２、８０３は、それぞれ個別のサービス加入者ごとの例である。例示した記録データには、それぞれ１０．１０．１０．１というアドレスを持つ端末から“brute-force”攻撃を受けたことが書かれている。しかし、検査システムによって統合された記録データ（８０４）では、個別の記録ではわからなかった新しい情報が得られる。図8の例の場合には、ＩＳＰが、検査サービス加入者を順番に攻撃していることがわかるため、攻撃を受けていないＩＳＰに接続しているユーザに警報を与えたり、より効果的な対処を施すことが可能になる。

【００４３】以上、本発明者によってなされた発明を、前記実施の形態に基づき具体的に説明したが、本発明は、前記実施の形態に限定されるものではなく、その要旨を逸脱しない範囲において種々変更可能であることは勿論である。

【００４４】

【発明の効果】本願において開示される発明のうち代表的なものによって得られる効果を簡潔に説明すれば、下記のとおりである。本発明によれば、ネットワークを利用するユーザは、セキュリティに関わるネットワーク機器を自ら設置することなく、インターネットに接続する際に利用するＩＳＰによって提供されるセキュリティソリューションを利用可能になる。

【００４５】すなわち、ユーザが攻撃の防御のためにハードウェアやソフトウェアを購入することなく、また、それらのハードウェアやソフトウェアを運用する知識を習得することなく、ネットワーク経由の攻撃を防ぐことができる。

【００４６】ＩＳＰの立場では、本発明をＩＳＰのサービスの付加価値として提供できることになる。

【００４７】ネットワークの帯域を消費するＤＤｏＳ（Distributed Denial of Service）のような攻撃を防御する場合には、本発明によれば、ＩＳＰがネットワークの接続形態の上流側から送られて来る好ましくないトラフィックを通過させないことを可能にし、これによって、ユーザがインターネット等の外部ネットワークへ接続するための帯域を確保することができるようになる。

【００４８】攻撃の検査サービスは、ＩＳＰ等のネットワーク運営者が一箇所で集中的に管理するシステムで提供するため、ユーザが個別で同様の攻撃検査をしていることに比べて、攻撃が行われた記録を収集できる範囲がＩＳＰ全体に広がる。このため、個別の記録だけではわからなかった新しい情報が得られることがある。

【図面の簡単な説明】

【図１】本発明の実施形態に係るネットワークの概略構成を示す模式図である。

【図２】本実施形態で実現されるトラフィックの流れの概要を説明するため模式図である。

【図３】本実施形態で実現される他のトラフィックの流れの概要を説明するための模式図である。

【図４】本実施形態の検査サーバの機能構成を示す図である。

【図５】本実施形態のエッジルータの処理手順を示すフローチャートである。

【図６】本実施形態のデータの検査を行うシステムの処理手順である。

【図７】本実施形態のデータの検査を行うシステムの処理例を説明するためのフローチャートである。

【図８】本実施形態の検査システムの動作を記録したデータである。

【符号の説明】

１００…インターネット

１０１、１０２、１０３…ユーザのネットワーク

１０４、１０５、１０６…ルータ　１０７…ＩＳＰのネットワーク

１０８…検査サーバ　１０９…ルータ

１１０、１１１…端末　２０１、２０２、２０３…端末

２０４…ルータ　２０５…検査サーバ

２１２…信頼できるネットワーク　２１３…信頼できないネットワーク

３０１…受信端末　３０２、３０３…端末

３０４、３０５…ルータ　３０６…検査サーバ

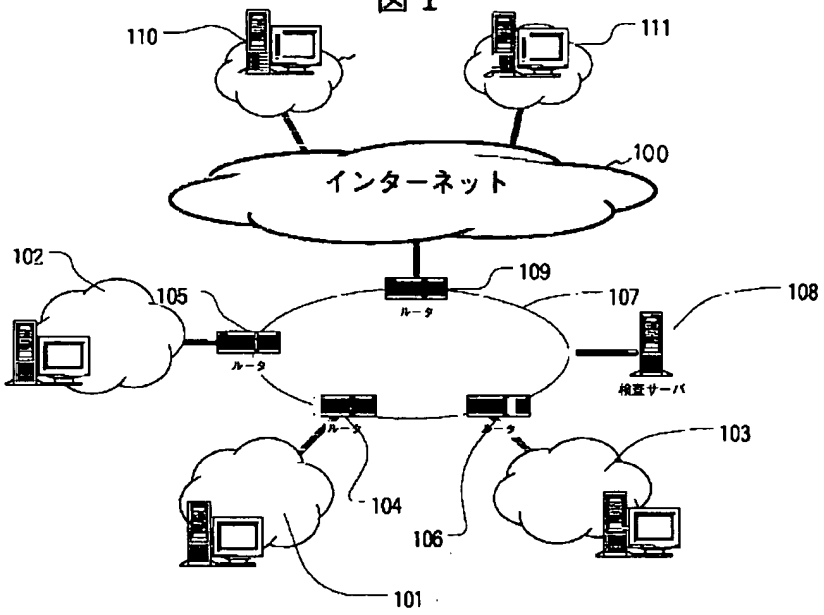
３１２…信頼できるネットワーク　３１３…信頼できないネットワーク

４０１…通信チャネル　４０２…ネット

ワークドライバ
４０３…データ分析部　　４０４…ユーザ
ポリシ実行部
４０５…侵入防御部　　４０６…ユーザ
データベース
４０７…侵入パターンデータベース　　４０８…加入者
管理部
４０９…ルーティング管理部　　５０１…端末
５０２…アクセステーブル

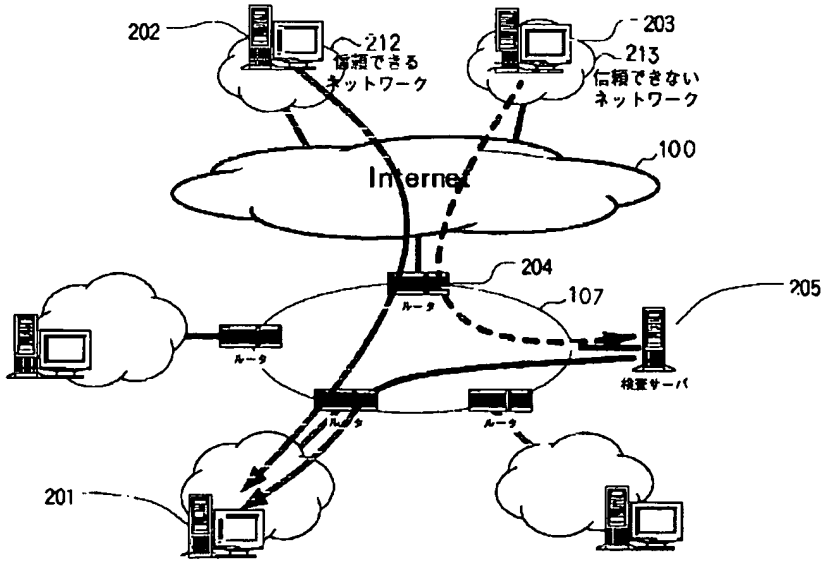
【図１】

図１



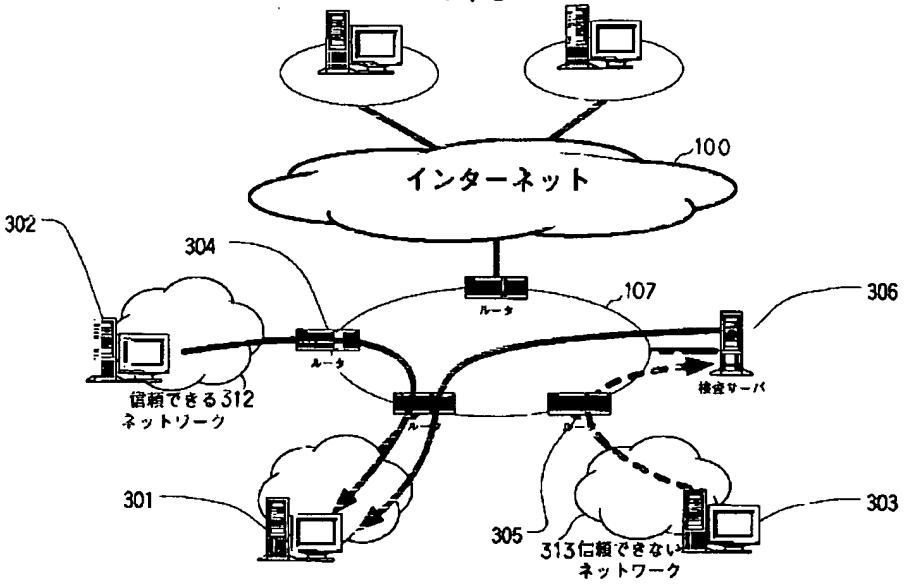
【図２】

図２



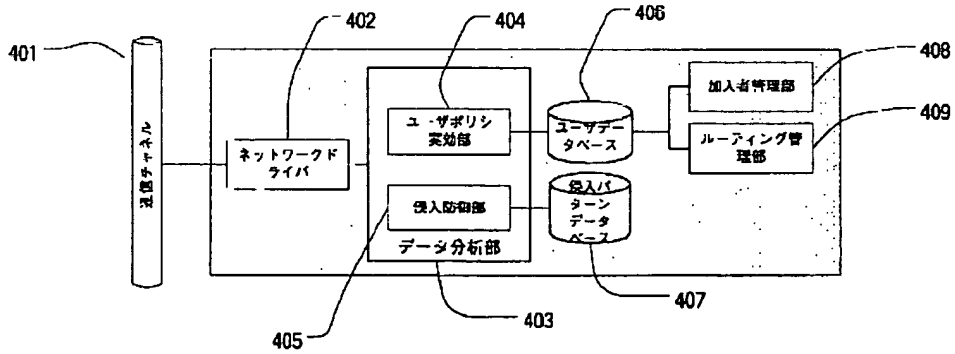
【図3】

図3


100
インターネット
302
304
107
306
ルータ
ルータ
検査サーバ
信頼できる312
ネットワーク
ルータ
ルータ
301
305
303
313信頼できない
ネットワーク

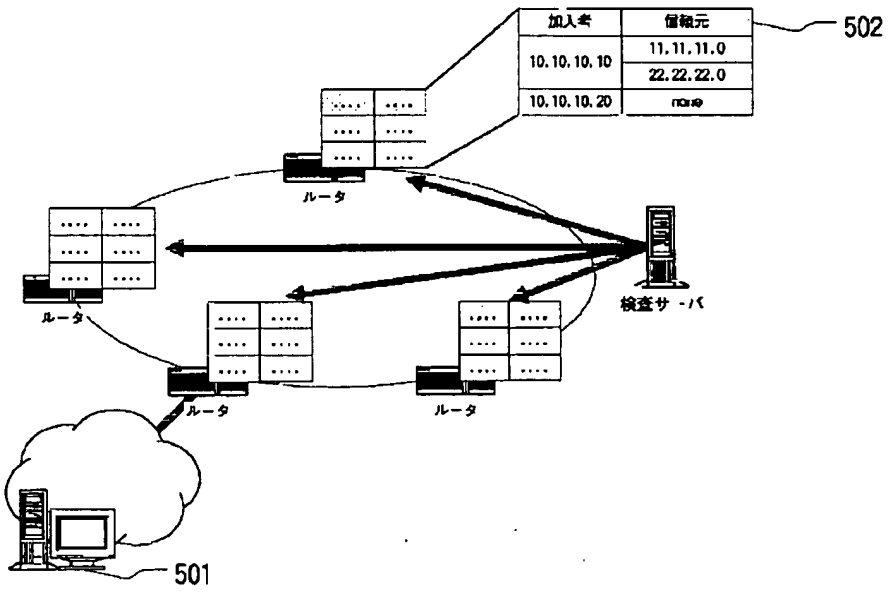
【図4】

図4


401
402
404
406
408
409
通信チャネル
ネットワークドライバ
ユーザポリシ実効部
ユーザデータベース
加入者管理部
ルーティング管理部
侵入防御部
侵入パターンデータベース
データ分析部
403
405
407

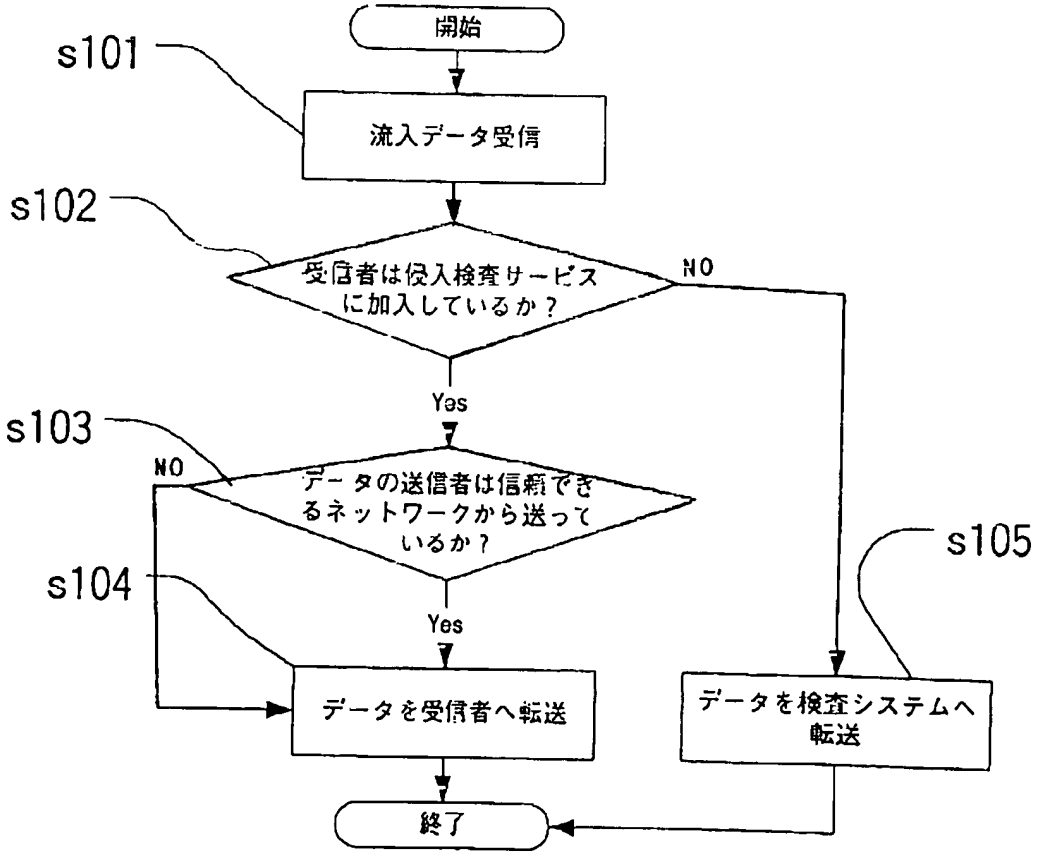
【図5】

図5


加入者
信頼元
10.10.10.10
11.11.11.0
22.22.22.0
10.10.10.20
502
ルータ
ルータ
ルータ
ルータ
検査サーバ
501

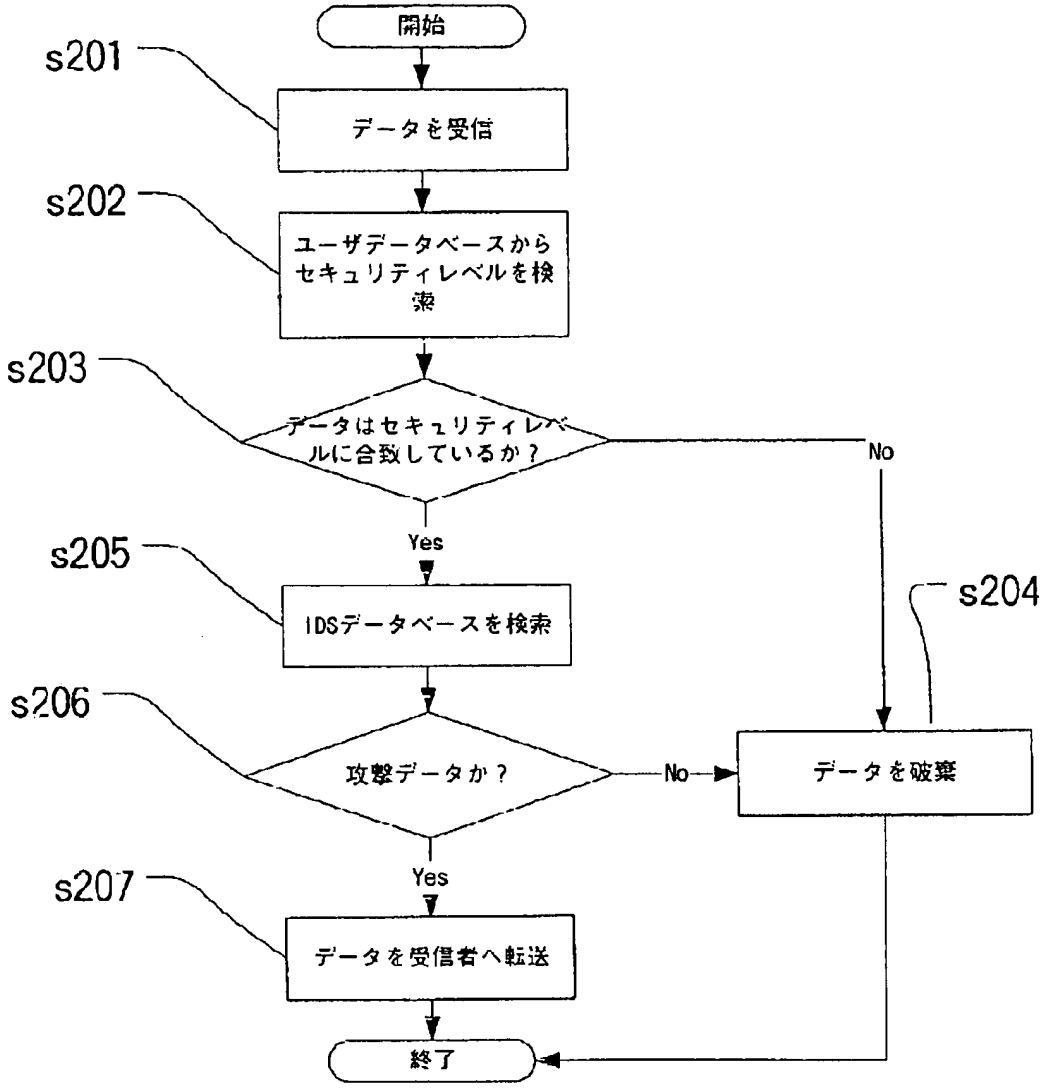
【図6】

図6


開始
s101
流入データ受信
s102
受信者は侵入検査サービスに加入しているか？
NO
Yes
s103
NO
データの送信者は信頼できるネットワークから送っているか？
s104
Yes
s105
データを受信者へ転送
データを検査システムへ転送
終了

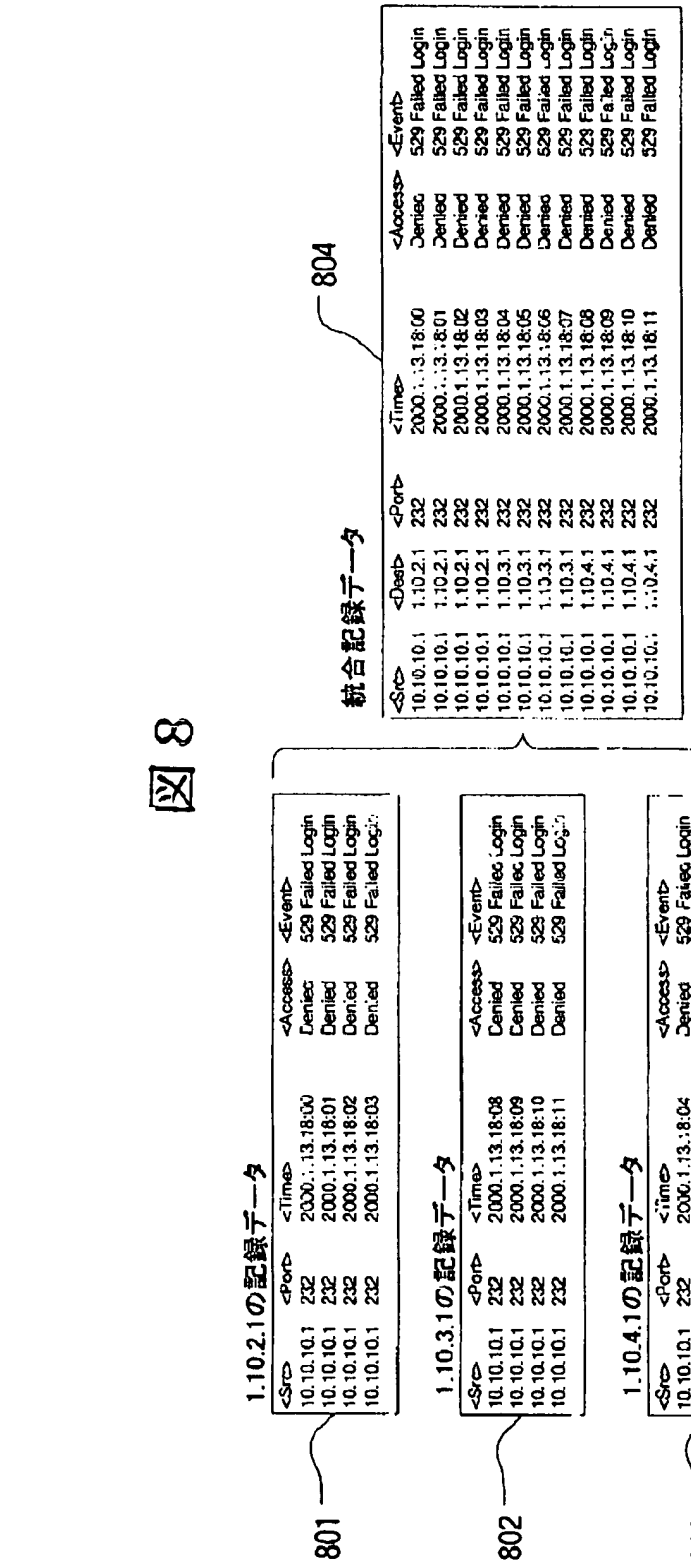
【図7】

図 7


開始
s201
データを受信
s202
ユーザデータベースからセキュリティレベルを検索
s203
データはセキュリティレベルに合致しているか？
No
Yes
s205
IDSデータベースを検索
s204
s206
攻撃データか？
No
データを破棄
Yes
s207
データを受信者へ転送
終了

【図8】

図8


1.10.2.1の記録データ
<Src> <Port> <Time> <Access> <Event>
10.10.10.1 232 2000.1.13.18:00 Denied 529 Failed Login
10.10.10.1 232 2000.1.13.18:01 Denied 529 Failed Login
10.10.10.1 232 2000.1.13.18:02 Denied 529 Failed Login
10.10.10.1 232 2000.1.13.18:03 Denied 529 Failed Login
801
1.10.3.1の記録データ
<Src> <Port> <Time> <Access> <Event>
10.10.10.1 232 2000.1.13.18:08 Denied 529 Failed Login
10.10.10.1 232 2000.1.13.18:09 Denied 529 Failed Login
10.10.10.1 232 2000.1.13.18:10 Denied 529 Failed Login
10.10.10.1 232 2000.1.13.18:11 Denied 529 Failed Login
802
1.10.4.1の記録データ
<Src> <Port> <Time> <Access> <Event>
10.10.10.1 232 2000.1.13.18:04 Denied 529 Failed Login
10.10.10.1 232 2000.1.13.18:05 Denied 529 Failed Login
10.10.10.1 232 2000.1.13.18:06 Denied 529 Failed Login
10.10.10.1 232 2000.1.13.18:07 Denied 529 Failed Login
803
804
統合記録データ
<Src> <Dest> <Port> <Time> <Access> <Event>
10.10.10.1 1.10.2.1 232 2000.1.13.18:00 Denied 529 Failed Login
10.10.10.1 1.10.2.1 232 2000.1.13.18:01 Denied 529 Failed Login
10.10.10.1 1.10.2.1 232 2000.1.13.18:02 Denied 529 Failed Login
10.10.10.1 1.10.2.1 232 2000.1.13.18:03 Denied 529 Failed Login
10.10.10.1 1.10.3.1 232 2000.1.13.18:04 Denied 529 Failed Login
10.10.10.1 1.10.3.1 232 2000.1.13.18:05 Denied 529 Failed Login
10.10.10.1 1.10.3.1 232 2000.1.13.18:06 Denied 529 Failed Login
10.10.10.1 1.10.3.1 232 2000.1.13.18:07 Denied 529 Failed Login
10.10.10.1 1.10.4.1 232 2000.1.13.18:08 Denied 529 Failed Login
10.10.10.1 1.10.4.1 232 2000.1.13.18:09 Denied 529 Failed Login
10.10.10.1 1.10.4.1 232 2000.1.13.18:10 Denied 529 Failed Login
10.10.10.1 1.10.4.1 232 2000.1.13.18:11 Denied 529 Failed Login

フロントページの続き

Fターム(参考) 5B089 GA04 GB02 KA17 KB04 KB13
5K030 GA15 HB19 HC01 HC14 HD03
HD06